Defense Message System
Medium Grade Services
(DMS/MGS)

ADMINISTRATOR DOCUMENTATION
FOR THE
CERTIFICATE PUBLICATION TOOL

Revision 1.02a (MITRE Corporation)
06-December-1999

Revision 1.03 (SRA/PRC)
13 March 2000

Prepared for:

DISA
Defense Information Systems Agency (D24)
5111 Leesburg Pike, 9th Floor
Falls Church, VA 22041

This documentation is designed to let an administrator quickly and easily deploy the Certificate Publication Tool on an Exchange server. This document will assume some basic knowledge of the operation and administration of Microsoft's Exchange Server as well as basic Windows NT navigation and administration skills.

1 Installation

The Certificate Publication Tool is comprised of the following files:

certpub.exe	-	main executable program
certpub.ini	-	sample configuration file
cpAccess.log	-	sample access log for runtime diagnostics
cpError.log	-	sample error log for runtime diagnostics
ads.exe	-	Active Directory Services installation program
qinstall.txt	-	quick installation guide and configuration reference
certpub.doc	-	this file

To install the tool, uncompress the archive into a suitable location. There is no installation wizard, so removal of the tool is accomplished by deleting the directory that the tool was installed into.

2 Preparation for Operation

In order for the tool to execute, the machine where it will be installed needs to have the Active Directory Services installed. This is accomplished by running the executable ads.exe included in the archive. The installation will copy a number of files to the system, and report on it’s success of failure. If there was a problem, make not of it and contact your Microsoft Technical Support liaison.

3 Configuration

Configuration of the tool is accomplished entirely through the configuration file, certpub.ini. The default contents of the file are shown in Figure 1. The only configuration value that must be specified is **certpubServer**. The rest of the values all have defaults hard-coded in the program that the configuration values override.

```
[certpubServer]
kelly.af.mil
[certpubUser]
kellyafb-certpub
[certpubSuccessSubject]
Success!
[certpubSuccessBody]
Your certificate has been published to the USAF GAL.
[certpubFailSubject]
Certificate publish request failed
[certpubFailBody]
Your attempt to publish a certificate to the GAL has
failed.\n\nPlease correct any errors and try again.
[certpubAccessLog]
cpAccess.log
[certpubErrorLog]
cpError.log
[certpubTempFile]
c:\temp\certpub.tmp
[certpubIndicatorValue]
Secured
[certpupDisplayIndicatorValue]
(PKI)
```

Figure 1 – certpub.ini configuration file contents

3.1 certpubServer

This controls the Exchange server that the tool will attempt to publish all requests to. It should be specified as the fully qualified hostname of the machine running the Exchange server. This attribute that must be set in the configuration file, no default value is provided since it will vary from site to site.

Default: *none*

3.2 certpubUser

This controls the user that the tool uses to connect to the Exchange server to retrieve publication requests as well as the user that the tool is set up to run as. A prior MAPI profile is not needed since one will be created on the fly whenever the tool is executed. This attribute that must be set in the configuration file, no default value is provided since it will vary from site to site.

Default: *none*
Recommended: <sitename>-certpub

3.3 certpubSuccessSubject

This defines the subject of the success message that will be sent when the tool successfully publishes a users digital certificate to the GAL.

Default: *Publishing Certificate to GAL Successful!*

3.4 certpubSuccessBody

This defines the message body for the success message that will be sent when the tool successfully publishes a users digital certificate to the GAL. To imbed returns into the body message, use the sequence of characters "\n" in the line specifying the body. The entire body must be specified on a single line.

Default: *Your DOD Certificate has been successfully published to the Global Address List.*

3.5 certpubFailSubject

This defines the subject of the failure message that will be sent when the tool encounters an error processing a user request.

Default: *Publishing Certificate to GAL Failed*

3.6 certpubFailBody

This defines the message body for the failure message that will be sent when the tool cannot publish a users digital certificate to the GAL. To imbed returns into the body message, use the sequence of characters "\n" in the line specifying the body. The entire body must be specified on a single line.

Default:

> *The Certificate Publisher failed to publish your certificate to the Global Address List. To send a signed email, do the following:*
>
> *Create a new message.*

*Address the message to the Certificate Publisher by either typing <**certpubUser**> on the To-Line, or choosing Certificate Publisher from the Global Address List.*

Digitally sign the message by choosing File, Properties from the menu bar. Click on the Security tab (if you do not have a security tab, you will need to enable security under Tools, Options.)

Check Add Digital Signature to Message. Ensure that Send Clear Text Signed Message is checked.

Click OK. Do not include any attachments with this message.

Click on the Send button.

If you have questions, please call the help desk.

3.7 certpubAccessLog

This setting defines the location and name of the access log. If only a file name is specified, the location will be relative to the location of the certpub.exe program. A full path may be specified.

Default: *cpAccess.log*

3.8 certpubErrorLog

This setting defines the location and name of the error log. If only a file name is specified, the location will be relative to the location of the certpub.exe program. A full path may be specified.

Default: *cpError.log*

3.9 certpubTempFile

This setting defines the location for the temporary file that is used to store the information extracted from the requestors email message.

Default: *certpub.tmp*

3.10 certpubIndicatorValue

This setting defines what value will be placed into Custom Attribute 5 and what will be seen in the user's exchange profile. If this value is not specified in the ini file then no value will be placed in the information store. This value will only be set if the certificate publication is successful.

Default: *Secured*

3.11 certpubDisplayIndicatorValue

This setting defines what will be appended onto the end of the display name. A space is automatically placed into the display name before this value is appended. If this value is not specified in the ini file then no value will be placed in the information store. The process will only occur if the certificate publication is successful.

Default: *(PKI)*

4 The Logging Facilities

The log files generated by the tool will allow an administrator to verify the successful operation of the tool as well as diagnose problems that may occur.

4.1 Accesses

The logging of accesses involves one line for every message that the tool processes, regardless of the success or failure of the processing. A sample access log line looks as follows:

```
[9/7/99 6:18:05 PM] - Processing message from /o=mitre.org/ou=ebola/cn=Recipients/cn=hendrick
```

The line is comprised of the date, a indicator message, and the sender of the message being processed.

4.2 Errors

The logging of errors involves one line for every error that occurs while processing a message. In general, a message is queued to the Bad folder on any error, so there will only be one error line for a given message. Samples of some of the errors logged are as follows:

```
[8/19/99 3:48:33 PM] - /o=mitre.org/ou=ebola/cn=Recipients/cn=hendrick - Incorrect number of
attachments - (0)
[8/19/99 4:02:08 PM] - /o=mitre.org/ou=ebola/cn=Recipients/cn=hendrick - Object doesn't support this
property or method
[8/19/99 4:08:09 PM] - /o=mitre.org/ou=ebola/cn=Recipients/cn=hendrick - Invalid message, subject not
empty
```

Like the accesses, the contents of an error line include the date, the sender of the message being processed (if known), and an error indicator.

4.3 Correlation of Accesses and Errors

In order to facilitate the correlation of access and errors, the tool generates the date string at the beginning of processing. This date string is used to log all messages regarding that particular message. It is therefore possible to match an error with an access to provide the capability of calculating the number of successful messages processed by the tool. This will not provide the number of unique messages processed, but it will give a good approximation since it is believed that most users will only publish their certificate on time. To further facilitate the correlation of accesses and errors, the administrator can choose to have a single log file for both accesses and errors. This is accomplished by specifying the same file for both the **certpubAccessLog** and **certpubErrorLog** settings in the configuration file

5 Exchange Server Configuration

5.1 Creating the Mailbox

A mailbox needs to be created that the tool can attach to receive and process user requests. In order to do this, make note of the **certpubUser** in the configuration file, this will be the mailbox name. The DMS-AF PMO has suggested that the mailbox name be of the form: <sitename>-certpub. Because of this, there is no default setting for the **certpubUser** setting.

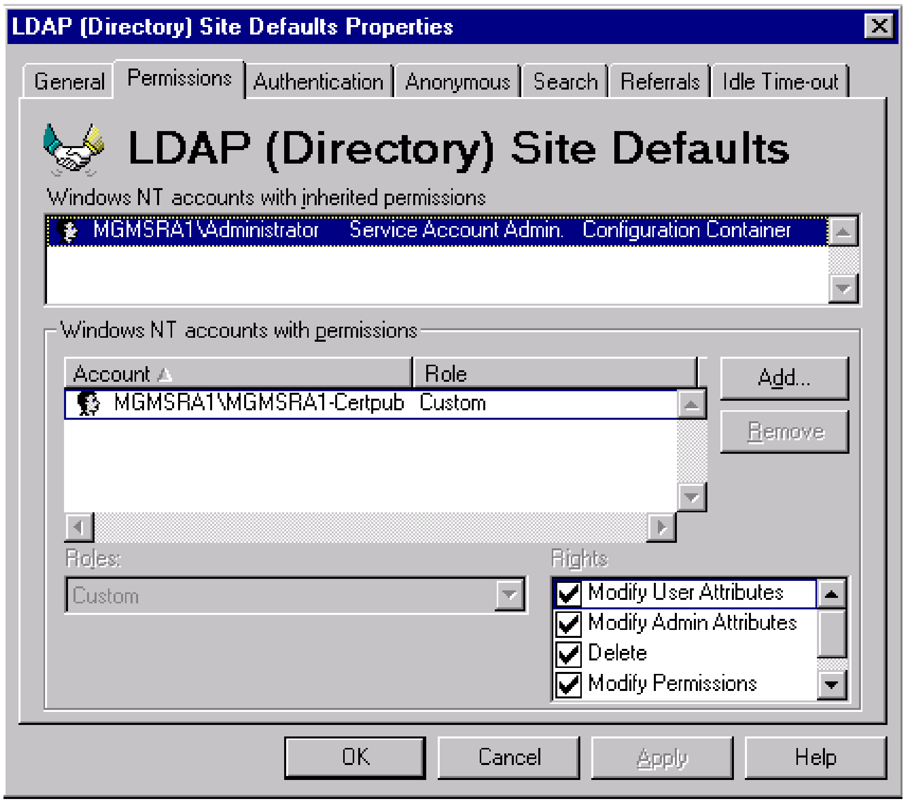
Follow the standard Exchange Server procedures for adding a new mailbox to the server. To minimize unauthorized access to the account, it is best if SMTP addressing is turned off for this mailbox. To do this, delete the SMTP address from the mailbox list of addresses. There should only be the X.400 Exchange Server address remaining. This will prevent non-Exchange users from sending mail to the account.

5.2 Setting Up a Limited Access User Account

To avoid any unnecessary potential for compromise of the Windows NT server that hosts the Exchange Server, it is best to run the tool as a non-privileged user. It is suggested that you use the same account as the mailbox where the users send their publication requests. These instructions are based on using the same account; change them accordingly if using a separate account.

This configuration will require that non-administrator access is granted to write to user accounts. To do this, make the following changes through the Exchange Administrator:

- Find the LDAP protocol settings (either site or local machine).
- Edit the properties for the LDAP protocol.
- Select the Permissions tab.
- Click "Add" to the right of the "Windows NT accounts with permissions" box.
- In the popup dialog box, select the same account as the owner of the tool mailbox and click OK.
- Make sure the permissions allowed for the account are:
    - Modify User Attributes
    - Search
- Click OK.



Windows NT accounts with inherited permissions

MGMSRA1\Administrator Service Account Admin. Configuration Container

Windows NT accounts with permissions

Account	Role
MGMSRA1\MGMSRA1-Certpub	Custom

Roles: Custom

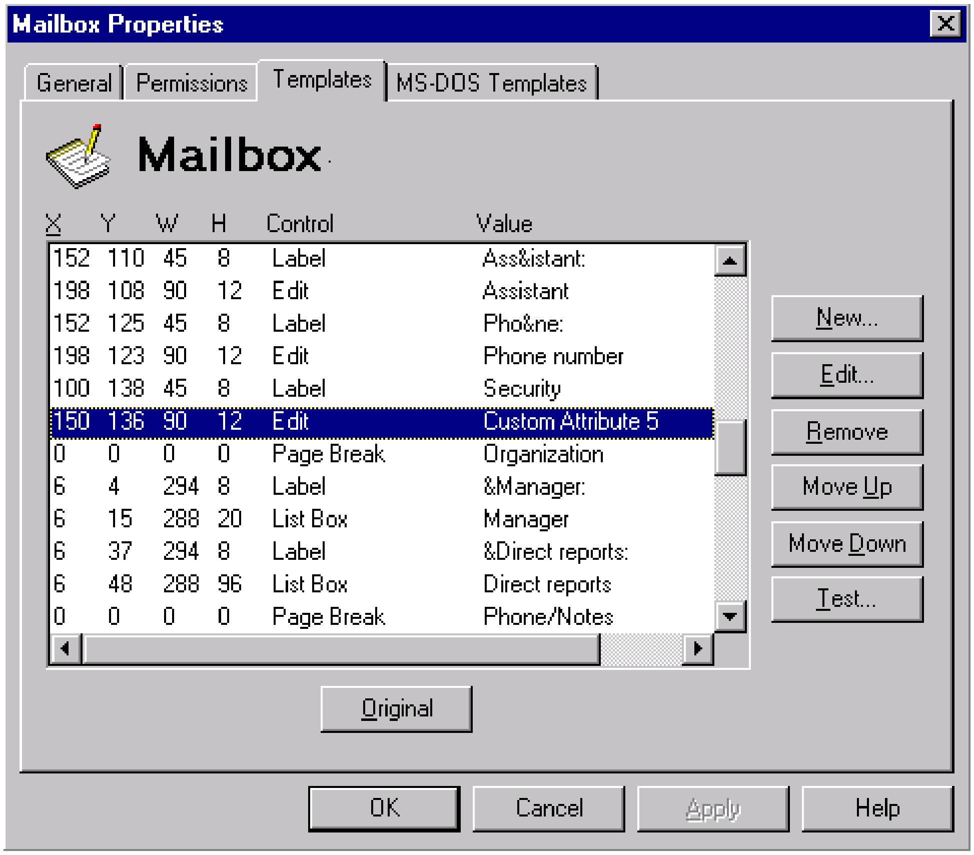
Rights:
☑ Modify User Attributes
☑ Modify Admin Attributes
☑ Delete
☑ Modify Permissions

5.3 Template Modifications for Certificate Visibility

In order to provide some indication to a user of the Global Address List (GAL) that another user has a certificate, an indicator has been added to the GAL when a user publishes their certificate. This attribute is hard coded in the certpub executable as Custom Attribute 5 (known as Extension-Attribute-5 internally to Exchange. The string that will be displayed to the user viewing an entry in the GAL is hard coded as “Secured”. These values are based on recommendations of the DMS-AF PMO.

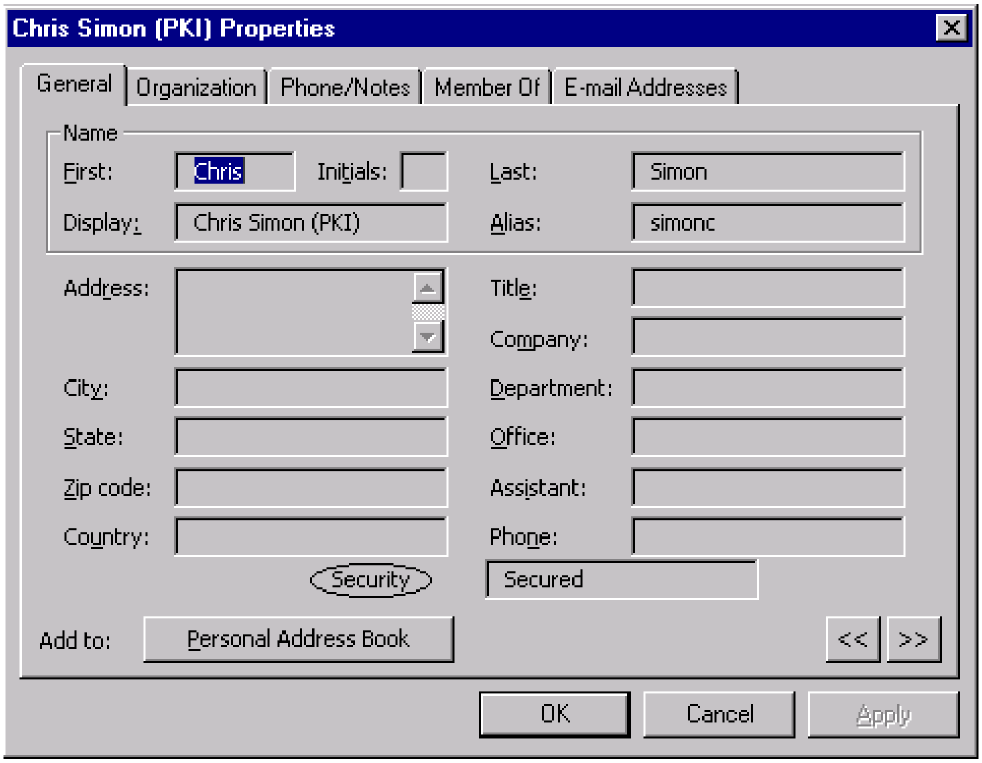
To modify the GAL template that a users sees when viewing a mailbox, open the Microsoft Exchange Administrator. From there, go to the server entry, Configuration, Addressing, Details Templates, English/USA, Mailbox entry. Edit the properties of the Mailbox entry as follows: [This is all based on the standard Mailbox Template. If the Template has been modified, the results may not be as expected. Some changes to the coordinates of the new entries may be needed to get it to line up properly.]

- Click on the Templates tab
- Highlight the entry that reads:
  0 0 0 0 Page Break Organization



X	Y	W	H	Control	Value
152	110	45	8	Label	Ass&istant:
198	108	90	12	Edit	Assistant
152	125	45	8	Label	Pho&ne:
198	123	90	12	Edit	Phone number
100	138	45	8	Label	Security
150	136	90	12	Edit	Custom Attribute 5
0	0	0	0	Page Break	Organization
6	4	294	8	Label	&Manager:
6	15	288	20	List Box	Manager
6	37	294	8	Label	&Direct reports:
6	48	288	96	List Box	Direct reports
0	0	0	0	Page Break	Phone/Notes

- Click New.
- Select Label.
- Set the coordinates as follows:
  X = 100, Y=138, W=45, H=8, text=Security
  [replace Security with whatever text you want the label to have]
- Click OK.
- Highlight the new entry.
- Click New.
- Select Edit.
- Set the values as follows:
  X=136, Y=136, W=90, H=12, Field=Custom Attribute 5, length=1024, Multiline=not checked
  [The Field is going to be one of the Custom Attributes, DMS-AF PMO recommends the use of Custom Attribute 5]
- Click OK.



Chris Simon (PKI) Properties

First: Chris
Initials:
Last: Simon
Display: Chris Simon (PKI)
Alias: simonc
Security: Secured
Add to: Personal Address Book

* The address book in Outlook will now contain the word “Security”, as shown above.

5.4 Replication of Sites with Certificate Publication Tool Running

A few motes need top be made regarding the use of the Certificate Publication Tool on sites that are replicated. To ensure against a mailbox collision, it is recommended that each site use a site-specific name for the publication mailbox. Figure 2 demonstrates a possible way to implement this recommendation.

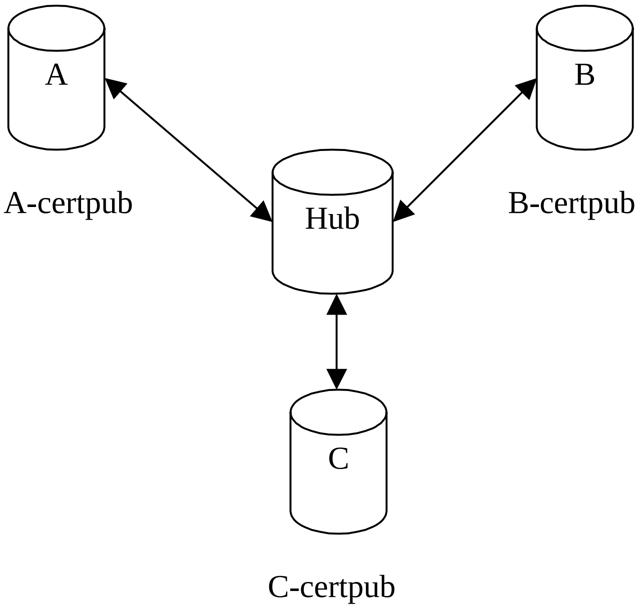


Figure 2 - if there are three sites in a replication strategy (A, B, and C, along with a replication hub), the corresponding mailbox names would be: A-certpub, B-certpub, and C-certpub.

Additionally, the default replication configuration does not include the userSMIMECertificate attribute (referred to internally to the Exchange server as Tagged-X509-Cert). For this attribute to be replicated among sites, it needs to be manually added to the list of attributes that are replicated. This is done via the Exchange Administrator by modifying the properties of the Directory Replication settings:

- In the Exchange Administrator double click on the site object
- Double click on “DS Site Configuration” object.
- Click on the “Attributes” tab
- In the field labeled “Configure” select “Inter-site replication”
- Scroll down and make sure that the attribute named “Tagged-X.509 Cert” is checked.

5.5 Client Configuration

In order for the end user to publish their certificate to the GAL, the client must be configured in two stages.

Stage One – Publishing

The client must send the signed message in clear text to the **<certpubUser>** mailbox. To do this the user must follow the procedure outlined below: (It is assumed here that the certificate is already locally installed on the client)

a. Go to the tools/options menu while still in the Inbox view – i.e. options that apply to the default settings of the client
b. Select the security tab
c. Make sure the box for "Add digital signature to outgoing messages" is checked
d. Make sure the box for "Send clear text signed messages" is checked
e. Send the message to the **<certpubUser>** mailbox
f. When the certificate is published successfully, the options set above must be cleared such that the default is not to add digital signatures to the outgoing messages. This is done by repeating steps A and B above then uncheck the boxes that were checked in steps C and D

Stage Two – Using the client for signing and encryption

This procedure is repeated on a per message basis as needed

a. Start a new message
b. Go to the View/options menu (or click on the options button in the toolbar)
c. To sign the message make sure the box for "Add digital signature to outgoing message" is checked
d. To encrypt the message make sure the box for "encrypt message contents and attachments" is checked